

Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.2, Avaya Aura® Session Manager R6.2 and Avaya Session Border Controller for Enterprise to support T-Mobile Vast Mobiel Integratie (Fixed Mobile Convergence) – Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the T-Mobile Vast Mobiel Integratie (Fixed Mobile Convergence) and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an Evolution Server. T-Mobile is a member of the DevConnect Service Provider program.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

NOTE: This Application Note is applicable with Avaya Aura® 6.2 which is currently in Controlled Introduction. Avaya Aura® 6.2 will be Generally Available in Summer 2012.

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between T-Mobile Vast Mobiel Integratie (Fixed Mobile Convergence) and an Avaya SIP-enabled Enterprise Solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise (Avaya SBCE), Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server. Customers using this Avaya SIP-enabled enterprise solution with the T-Mobile Vast Mobiel Integratie service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the Enterprise customer.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Communication Manager, Session Manager and Session Border Controller for Enterprise. The enterprise site was configured to use the SIP Trunk service provided by T-Mobile.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from the PSTN routed to the DDI numbers assigned by T-Mobile
- Incoming PSTN calls made to SIP, H.323 and Analogue telephones at the enterprise
- Outgoing calls from the enterprise site completed via T-Mobile to PSTN destinations
- Outgoing calls from the enterprise to the PSTN made from SIP, H.323 and Analogue telephones
- Calls using the G.711A, G.729A and G.729B codecs
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- User features such as hold and resume, transfer, conference, call forwarding, etc
- Caller ID Presentation and Caller ID Restriction
- Direct IP-to-IP media (also known as "shuffling") with SIP and H.323 telephones
- Call coverage and call forwarding for endpoints at the enterprise site
- Transmission and response of SIP OPTIONS messages sent by T-Mobile requiring Avaya response and sent by Avaya requiring T-Mobile response

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the T-Mobile Vast Mobiel Integratie service with the following observations:

- No inbound toll free numbers were tested as none were available from the Service Provider
- No Emergency Services numbers were tested as test calls to these numbers should be prearranged with the Operator
- Configuration required to keep SIP messages under 1500 bytes as fragmented SIP messages were not being re-assembled at the network
- The network responds to re-INVITES from the enterprise to initiate T38 fax transmission with 488 "Not Accepted Here", accepted as fax is not supported for this service
- When pass-through fax is used and initial voice set-up is with G.729, the network attempts to re-negotiate with T.38 and fax transmission fails.
- When CLI is restricted, the user part of the From and P-Asserted-ID fields is set to "anonymous" and the Privacy header is not sent. In this case, the enterprise equipment does not correctly indicate that the caller is "Private".

2.3. Support

For support from T-Mobile Netherlands on configuration, please contact the Sales Implementation Manager at T-Mobile.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the T-Mobile Vast Mobiel Integratie service. Located at the Enterprise site is a Session Border Controller, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 46xx series IP telephones (with H.323 firmware), Avaya 16xx series IP telephones (with SIP firmware) Avaya A175 Desktop Video Device running Flare Experience, Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone running on a laptop PC configured for H.323.

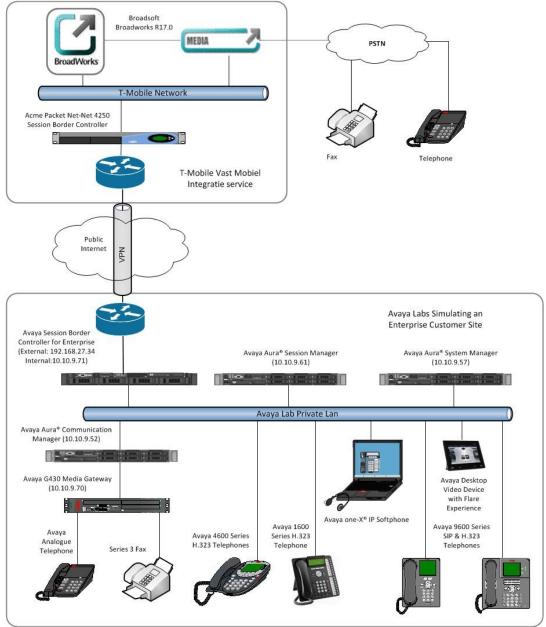


Figure 1: T-Mobile SIP Solution Topology

Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved. 4 of 47 TMOB_CM62SBC

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya S8800 Server	Avaya Aura® Communication Manager
	R6.2
	(R016x.02.0.823.0)
Avaya G430 Media Gateway	FW 30.12.1
Avaya S8800 Server	Avaya Aura® Session Manager R6.2
	(6.2.0.0.620120)
Avaya S8800 Server	Avaya Aura® System Manager R6.2
	(System Platform 6.2.0.0.27, Template
	6.2.12.0)
Dell R210 V2 Server	Avaya Session Border Controller for
	Enterprise 4.0.5.Q02
Avaya 1616 Phone (H.323)	1.301
Avaya 4621 Phone (H.323)	2.902
Avaya 9630 Phone (H.323)	3.103
Avaya A175 Desktop Video Device (SIP)	Flare Experience Release 1.1
Avaya 9630 Phone (SIP)	R2.6 SP6
Avaya one-X® Communicator (H.323) on	Avaya one-X® Communicator
Lenovo T510 Laptop PC	6.1.3.08-SP3-Patch2-35791
Analogue Phone	N/A
T-Mobile	
SBC - ACME Net-Net 4250	Firmware C5.1.1 Patch 28 (Build 629)
CPE - Cisco 1921	c1900-universalk9-mz.SPA.151-4.M3.bin
Application server – BroadSoft	BroadWorks R17.0
BroadWorks	

Note: At the time of test, Communication Manager R6.2 was in the Control Introduction phase prior to being made GA.

5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP Signalling associated with the T-Mobile Vast Mobiel Integratie service. For incoming calls, the Session Manager receives SIP messages from the Avaya Session Border Controller for Enterprise and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions.

Once Communication Manager selects a SIP trunk, the SIP signalling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the Session Border Controller at the enterprise site that then sends the SIP messages to the T-Mobile network. Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. The general installation of the Avaya S8800 Servers and Avaya G430 Media Gateway is presumed to have been previously completed and is not discussed here.

5.1. Confirm System Features

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Use the **display system-parameters customer-options** command and on **Page 2**, verify that the **Maximum Administered SIP Trunks** supported by the system is sufficient for the combination of trunks to the T-Mobile network, and any other SIP trunks used.

display system-parameters customer-options	Pag	e 2 o	f 11	
OPTIONAL FEATURES				
IP PORT CAPACITIES	USED			
Maximum Administered H.323 Trunks:	12000 0			
Maximum Concurrently Registered IP Stations:	18000 3			
Maximum Administered Remote Office Trunks:	12000 0			
Maximum Concurrently Registered Remote Office Stations:	18000 0			
Maximum Concurrently Registered IP eCons:	414 0			
Max Concur Registered Unauthenticated H.323 Stations:	100 0			
Maximum Video Capable Stations:	18000 0			
Maximum Video Capable IP Softphones:	18000 0			
Maximum Administered SIP Trunks:	24000 12			
Maximum Administered Ad-hoc Video Conferencing Ports:	24000 0			
Maximum Number of DS1 Boards with Echo Cancellation:	522 0			
Maximum TN2501 VAL Boards:	128 0			
Maximum Media Gateway VAL Sources:	250 1			
Maximum TN2602 Boards with 80 VoIP Channels:	128 0			
Maximum TN2602 Boards with 320 VoIP Channels:	128 0			
Maximum Number of Expanded Meet-me Conference Ports:	300 0			

On Page 4, verify that the IP Trunks field is set to y.

```
display system-parameters customer-options
                                                                      4 of 11
                                                               Page
                               OPTIONAL FEATURES
                                                                IP Stations? y
   Emergency Access to Attendant? y
          Enable 'dadmin' Login? y
          Enhanced Conferencing? y
                                                          ISDN Feature Plus? n
                                        ISDN/SIP Network Call Redirection? y
                Enhanced EC500? y
   Enterprise Survivable Server? n
                                                            ISDN-BRI Trunks? y
      Enterprise Wide Licensing? n
                                                                   ISDN-PRI? y
                                                 Local Survivable Processor? n
             ESS Administration? y
         Extended Cvg/Fwd Admin? y
                                                       Malicious Call Trace? y
    External Device Alarm Admin? y
                                                   Media Encryption Over IP? n
                                      Mode Code for Centralized Voice Mail? n
 Five Port Networks Max Per MCC? n
               Flexible Billing? n
  Forced Entry of Account Codes? y
                                                   Multifrequency Signaling? y
     Global Call Classification? y
                                          Multimedia Call Handling (Basic)? y
                                        Multimedia Call Handling (Enhanced)? y
           Hospitality (Basic)? y
 Hospitality (G3V3 Enhancements)? y
                                                 Multimedia IP SIP Trunking? y
                      IP Trunks? y
          IP Attendant Consoles? y
```

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **SM100** and **10.10.9.61** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** name as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

display node-name	es ip	
		IP NODE NAMES
Name	IP Address	
SM100	10.10.9.61	
Sipera-SBC	10.10.9.71	
default	0.0.0.0	
procr	10.10.9.52	
procr6	::	

5.3. Administer IP Network Region

Use the **change ip-network-region 1** command to set the following values:

- The Authoritative Domain field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**.
- By default, **IP-IP Direct Audio** (both **Intra-** and **Inter-Region**) is enabled (**yes**) to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. When a PSTN call is shuffled, the media stream is established directly between the enterprise end-point and the internal media interface of the Avaya SBCE.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set 1 is used.

```
change ip-network-region 1
                                                               Page 1 of 20
                              IP NETWORK REGION
 Region: 1
Location: 1
              Authoritative Domain: avaya.com
   Name: default
MEDIA PARAMETERS
                               Intra-region IP-IP Direct Audio: yes
                               Inter-region IP-IP Direct Audio: yes
     Codec Set: 1
  UDP Port Min: 2048
                                         IP Audio Hairpinning? n
  UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
       Audio PHB Value: 46
       Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
       Audio 802.1p Priority: 6
       Video 802.1p Priority: 5
                                     AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS
                                                       RSVP Enabled? n
 H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
           Keep-Alive Count: 5
```

5.4. Administer IP Codec Set

Open the **IP Codec Set** form for the codec set specified in the IP Network Region form, **Section 5.3.** Enter the list of audio codecs eligible to be used in order of preference. For the interoperability test the codecs supported by T-Mobile were configured, namely **G.729A**, **G.729B** and **G.711A**.

change ip-codec	-set 1			Page	1 of	2
	IP					
Codec Set:	1					
Audio Codec 1: G.729A 2: G.729B 3: G.711A 4:	Silence Suppression n n n	Frames Per Pkt 2 2 2 2	Packet Size(ms) 20 20 20			

The T-Mobile Vast Mobiel Integratie service does not currently support T.38 for transmission of fax. Although not supported as a standard configuration by Avaya, G.711 pass-through was tested. To set G.711 pass-through, navigate to **Page 2** and configure by setting the **Fax Mode** to **pass-through** as shown below.

```
change ip-codec-set 1
                                                                          2 of
                                                                   Page
                                                                                  2
                           IP Codec Set
                               Allow Direct-IP Multimedia? n
                    Mode
                                         Redundancy
                    pass-through
    FAX
                                          1
    Modem
                     off
                                          0
    TDD/TTY
                     US
                                          3
                                          0
    Clear-channel
                     n
```

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the T-Mobile Vast Mobiel Integratie service. During test, this was configured to use **TCP** and port **5060** to facilitate tracing and fault analysis. It is recommended however, to use TLS (Transport Layer Security) and the default TLS port of **5061** for security. Configure the **Signaling Group** using the **add signaling-group x** command, where **x** is an available signalling group, as follows:

- Set Group Type to sip
- Set Transport Method to tcp
- Set **Peer Detection Enabled** to y allowing the Communication Manager to automatically detect if the peer server is a Session Manager
- Set Near-end Node Name to the processor interface (node name procr as defined in the IP Node Names form shown in Section 5.2)
- Set Far-end Node Name to the Session Manager (node name SM100 as defined in the IP Node Names form shown in Section 5.2)
- Set Near-end Listen Port and Far-end Listen Port to 5060 (Commonly used TCP port value)
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3**. (logically establishes the far-end for calls using this signalling group as network region 1)
- Leave **Far-end Domain** blank (Allows the CM to accept calls from any SIP domain on the associated trunk)
- Set Direct IP-IP Audio Connections to y
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager)

The default values for the other fields may be used.

```
change signaling-group 1
                                                            Page 1 of 2
                              SIGNALING GROUP
Group Number: 1
                           Group Type: sip
 IMS Enabled? n
                      Transport Method: tcp
      Q-SIP? n
    IP Video? n
                                               Enforce SIPS URI for SRTP? y
 Peer Detection Enabled? y Peer Server: SM
                                          Far-end Node Name: SM100
  Near-end Node Name: procr
Near-end Listen Port: 5060
                                       Far-end Listen Port: 5060
                                    Far-end Network Region: 1
Far-end Domain:
                                         Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate
                                          RFC 3389 Comfort Noise? n
       DTMF over IP: rtp-payload
                                         Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3
                                                   IP Audio Hairpinning? n
 Enable Layer 3 Test? y
                                              Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n
                                              Alternate Route Timer(sec): 6
```

5.6. Administer SIP Trunk Group

A trunk group is associated with the signaling group described in Section 5.5. Configure the trunk group using the add trunk-group x command, where x is an available trunk group. On Page 1 of this form:

- Set the Group Type field to sip
- Choose a descriptive Group Name
- Specify a trunk access code (TAC) consistent with the dial plan
- The **Direction** is set to **two-way** to allow incoming and outgoing calls
- Set the **Service Type** field to **public-netwrk** required setting when using the Diversion header
- Specify the signalling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**
- Specify the Number of Members supported by this SIP trunk group

```
      add trunk-group 1
      Page 1 of 21

      TRUNK GROUP
      TRUNK GROUP

      Group Number: 1
      Group Type: sip CDR Reports: y

      Group Name: Group 1
      COR: 1

      Direction: two-way
      Outgoing Display? y

      Dial Access? n
      Night Service:

      Queue Length: 0
      Auth Code? n

      Service Type: public-ntwrk
      Auth Code? n

      Member Assignment Method: auto
      Signaling Group: 1

      Number of Members: 10
```

On **Page 2** of the trunk-group form, the Preferred **Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed upon with T-Mobile to prevent unnecessary SIP messages during call setup.

```
Add trunk-group 1

Group Type: sip

TRUNK PARAMETERS

Unicode Name: auto

Redirect On OPTIM Failure: 5000

SCCAN? n

Digital Loss Group: 18

Preferred Minimum Session Refresh Interval(sec): 600

Disconnect Supervision - In? y Out? y
```

On **Page 3**, set the **Numbering Format** field to **private**. This allows delivery of CLI in national format with a leading 0.

```
add trunk-group 1 Page 3 of 21
TRUNK FEATURES
ACA Assignment? n Measured: none
Maintenance Tests? y
Numbering Format: private
UUI Treatment: service-provider
Replace Restricted Numbers? n
Replace Unavailable Numbers? n
```

On Page 4 of this form:

- Set **Support Request History** to **n** as T-Mobile does not use History Info making it an unnecessary extension to the SIP INVITE
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by T-Mobile
- Set the **Convert 180 to 183 for Early Media** to **y**, this is not necessary but was set during test so is shown here
- Set Always Use re-INVITE for Display Updates to y to allow correct operation of fax

```
add trunk-group 1

PROTOCOL VARIATIONS

Mark Users as Phone? n

Prepend '+' to Calling Number? n

Send Transferring Party Information? n

Network Call Redirection? y

Send Diversion Header? n

Support Request History? n

Telephone Event Payload Type: 101

Convert 180 to 183 for Early Media? y

Always Use re-INVITE for Display Updates? y

Identity for Calling Party Display: P-Asserted-Identity

Enable Q-SIP? n
```

5.7. Administer Calling Party Number Information

Use the **change private-unknown-numbering** command to configure Communication Manager to send the calling party number. In the test configuration, individual stations were mapped to send numbers allocated from the T-Mobile DDI range supplied. This calling party number is sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones. Note that the digits identifying the DDI range are not shown.

char	nge private-numb	bering 0				Page	1 of	E 2	
		NUI	MBERING - PRIVATE	FORMAI	1				
Ext	Ex+	Trk	Private	Total					
-									
Len	Code	Grp(s)	Prefix	Len					
4	2000	1	018xxxxxx9	10	Total Admir	nistered	: 7		
4	2296	1	018xxxxx7	10	Maximum	Entries	: 54	10	
4	2316	1	018xxxxxx9	10					
4	2346	1	018xxxxx6	10					
4	2396	1	018xxxxxx5	10					
4	2400	1	018xxxxxx9	10					
4	2601	1	018xxxxx8	10					

5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to the T-Mobile Vast Mobiel Integratie service. The single digit **9** was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line. Use the **change feature-access-codes** command to configure a digit as the **Auto Route Selection (ARS) - Access Code 1**.

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to numbers beginning 0 or 00. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 1**.

change ars analysis 0	ΔE	S DIG	IT ANALYS	IS TABLE		Page 1 of 2
	211		Location:		_	Percent Full: 0
Dialed	Tot	al	Route	Call	Node	ANI
String	Min	Max	Pattern	Type	Num	Reqd
0	8	14	1	pubu		n
00	13	17	1	pubu		n
00353	10	14	1	pubu		n
0044	12	14	1	pubu		n
01	7	14	1	pubu		n
01989	5	7	1	pubu		n
0221	12	14	1	pubu		n
0800	11	11	1	pubu		n
118	5	6	1	pubu		n

Use the **change route-pattern x** command, where **x** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern 1 is used to route calls to trunk group 1. Set the **Numbering Format** to **unk-unk**.

cha	nge	rout	e-pa	tter	n 1]	Page	1	of	3	
					Pat	tern 1	Numbei	c: 1	Patt	ern Nam	ne:	all	cal	ls					
							SCCAN	J? n	Se	ecure Sl	IP?	n							
	Grp	FRL	NPA	Pfx	Нор	Toll	No.	Inse	rted							DC	cs/	IXC	
	No			Mrk	Lmt	List	Del	Digit	ts							QS	SIG		
							Dqts	2								Ir	ntw		
1:	1	0					-									r	ı	user	
2:																r	ı	user	
3:																r	ı	user	
4:																r	ı	user	
5:																r	ı	user	
6:																r	1	user	
	BC	C VA	LUE	TSC	CA-	TSC	ITC	BCIE	Servi	ice/Feat	ture	PAF	RM I	No.	Numb	erir	ng 1	LAR	
	0 1	2 M	4 W		Req	uest							D	gts	Form	at	-		
					-							S	Suba	ddre	ess				
1:	УУ	УУ	уn	n			rest	5							unk-	unk	1	none	
2:	УУ	уу	уn	n			rest	5									1	none	
3:	УУ	УУ	y n	n			rest	5									1	none	
4:	УУ	УУ	уn	n			rest	5									1	none	
5:	УУ	УУ	уn	n			rest	5									1	none	
6:	УУ	УУ	уn	n			rest	5									1	none	

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from T-Mobile can be manipulated as necessary to route calls to the desired extension. In the example, the incoming DDI numbers provided by T-Mobile for testing are assigned to the internal extensions of the test equipment configured within the Communication Manager. The **change inc-call-handling-trmt trunk-group 1** command is used to translate numbers **018nnnnn5** to **018nnnnn9** to the 4 digit extension by deleting **all** of the incoming digits and inserting the extension number. Note that the significant digits beyond the city code have been obscured.

change inc-cal	l-handli:	ng-trmt tr	unk-grou	p 1	Page	1 of	30	
		INCOMING	CALL HANI	DLING TREATMENT				
Service/	Number	Number	Del 1	Insert				
Feature	Len	Digits						
public-ntwrk	10 01	8nnnnn5	all	2396				
public-ntwrk	10 01	8nnnnnn6	all	2346				
public-ntwrk	10 01	8nnnnn7	all	2296				
public-ntwrk	10 01	8nnnnn8	all	2601				
public-ntwrk	10 01	8nnnnnn9	all	2000				
public-ntwrk								

5.10. EC500 Configuration

When EC500 is enabled on the Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 2396. Use the command **change off-pbx-telephone station mapping x** where **x** is the Communication Manager station.

- The Station Extension field will automatically populate with station extension
- For Application enter EC500
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration
- For the **Phone Number** enter the phone that will also be called (e.g. **0035386xxxxxx**)
- Set the **Trunk Selection** to **1** so that Trunk Group 1 will be used for routing
- Set the **Config Set** to **1**

change off-pbx	-telephone st	ation-mapp	ing 2396		Page 1	of 3	3
	STATIONS	WITH OFF-P	BX TELEPHONE INT	EGRATION			
Station Extension 2396	Application EC500	Dial CC Prefix - -	Phone Number 00353867818306	Trunk Selection 1	Config Set 1	Dual Mode	

Save Communication Manager changes by entering save translation to make them permanent.

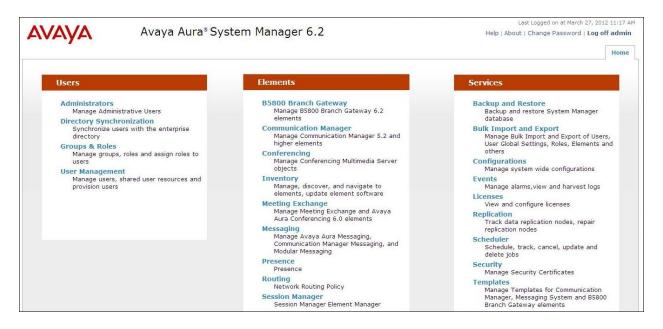
6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The Session Manager is configured via the System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer Locations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Application for Avaya Aura® Communication Manager
- Administer Application Sequence for Avaya Aura® Communication Manager
- Administer SIP Extensions

6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a Web Browser by entering http://<FQDN >/SMGR, where <FQDN> is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the Home tab will be presented with menu options shown below.



6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name (e.g., **avaya.com**) and optionally a description for the domain in the **Notes** field. Click **Commit** to save changes.

AVAYA	Avaya Aura [®] System Mana		Last Logged on at March 29, 2012 10:41 A It Change Password Log off admin		
					Routing * Home
* Routing	Home /Elements / Routing / Domains				
Domains					Help ?
Locations	Domain Management				
Adaptations	Edit New Duplicate Delete	More Actions			
SIP Entities	Eait New Dupicate Delete	More Accors	h		
Entity Links	2 Items Refresh				Filter: Enable
Time Ranges					Filter: Enable
Routing Policies	Name Name	Туре	Default	Notes	
Dial Patterns	avaya.com	sip			
Regular Expressions	test.com	sip			
Defaults	Select : All, None				

6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside, for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. On the **Routing** tab select **Locations** from the left hand menu. Under **General**, in the **Name** field, enter an informative name for the location. Scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, * is used to specify any number of allowed characters at the end of the string. Below is the location configuration used for the test enterprise.

Home /Elements / Routing / Locations			
			Help ?
Location Details			Commit Cancel
General			
* Name:	Galway		
Notes:			
Overall Managed Bandwidth			
Managed Bandwidth Units:	Kbit/sec 💌		
Total Bandwidth:			
Multimedia Bandwidth:			
Audio Calls Can Take Multimedia Bandwidth:			
Per-Call Bandwidth Parameters			
Maximum Multimedia Bandwidth (Intra-Location):	1000 Kbit/Sec		
Maximum Multimedia Bandwidth (Inter-Location):	1000 Kbit/Sec		
* Minimum Multimedia Bandwidth:	64 Kbit/Sec		
* Default Audio Bandwidth:	80 Kbit/sec 💌		
Alarm Threshold			
Overall Alarm Threshold:	80 🖌 %		
Multimedia Alarm Threshold:	80 💉 %		
* Latency before Overall Alarm Trigger:	5 Minutes		
* Latency before Multimedia Alarm Trigger:	5 Minutes	\searrow	
Location Pattern			
Add Remove			
3 Items Refresh			Filter: Enable
IP Address Pattern		Notes	
* 10.10.9.*		Private	

6.4. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to the Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity. Under **General**:

- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **Gateway** for the Session Border Controller SIP entity
- In the Location field select the appropriate location from the drop down menu
- In the **Time Zone** field enter the time zone for the SIP Entity

In this configuration there are three SIP Entities:

- Avaya Aura® Session Manager SIP Entity
- Avaya Aura® Communication Manager SIP Entity
- Avaya Session Border Controller for Enterprise SIP Entity

6.4.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signalling interface. The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these, scroll to the bottom of the page and under **Port**, click **Add**, then edit the fields in the resulting new row.

- In the **Port** field enter the port number on which the system listens for SIP requests
- In the **Protocol** field enter the transport protocol to be used for SIP requests
- In the **Default Domain** field, from the drop down menu select **avaya.com** as the default domain

Home /Elements / Routing / SIP Entities			
SIP Entity Details		Help Commit Cance	0.000
General			-84
	Session Manager		
* FQDN or IP Address:			
	Session Manager		
Notes:			
Location:	Galway 💌		
Outbound Proxy:	~		
Time Zone:	Europe/Dublin		
Credential name:			
SIP Link Monitoring	Use Session Manager Configuration 👻		
Entity Links			
Add Remove			
2 Items Refresh		Filter: Enable	е
SIP Entity 1 Protocol Port	SIP Entity 2	Port Connection Policy	
Session Manager 💙 TCP 💌 * 50	50 Communication Manager 😪	* 5060 Trusted 💌	
Session Manager 🗸 TCP 💌 * 50	50 Sipera SBC 💌	* 5060 Trusted 💌	
Select : All, None			
Port			
TCP Failover port:			
Add Remove		N	
		R	-
3 Items Refresh		Filter: Enable	2
	t Domain Notes		
5060 TCP 💌 avaya.			
5060 UDP w avaya. 5061 TLS v avaya.			
			-
Select : All, None			

Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved.

6.4.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling.

Home /Elements / Routing / SIP Entities	
	Help ?
SIP Entity Details	Commit Cancel
General	
* Name:	Communication Manager
* FQDN or IP Address:	10.10.9.52
Type:	CM M
Notes:	
Adaptation:	×
Location:	Galway 💌
Time Zone:	Europe/Dublin
Override Port & Transport with DNS SRV:	
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none 💌
SIP Link Monitoring	
	Use Session Manager Configuration 💌

6.4.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP Entity for the Session Border Controller. The **FQDN or IP** Address field is set to the IP address of the Session Border Controller private network interface.

Home /Elements / Routing / SIP Entities		
		Help ?
SIP Entity Details		Commit Cancel
General		
* Name:	Sipera SBC	
* FQDN or IP Address:	10.10.9.71	
Type:	Gateway	
Notes:		
Adaptation:	V	
Location:	Galway 💌	
Time Zone:	Europe/Dublin	
Override Port & Transport with DNS SRV:		
* SIP Timer B/F (in seconds):	4	
Credential name:		
Call Detail Recording:	none 💌	
SIP Link Monitoring		
SIP Link Monitoring:	Use Session Manager Configuration 💌	

Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved.

6.5. Administer Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- In the Name field enter an informative name
- In the SIP Entity 1 field select Session Manager
- In the **Port** field enter the port number to which the other system sends its SIP requests
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.4**
- In the **Port** field enter the port number to which the other system expects to receive SIP requests
- In the **Connection Policy** field enter **Trusted** to make the other system trusted
- In the **Protocol** field enter the transport protocol to be used to send SIP requests

Click **Commit** to save changes. The following screen shows the Entity Links used in this configuration.

	/Elements / Routing / Entity Links							
ntity	Links							Help
Edit	New Duplicate Delete More	Actions •						
2 Itei	ms Refresh	Planet setures - A	Protocol	Port	STP Entity 2	Port		: Enable
2 Itei	ms Refresh Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	: Enable Notes
	ms Refresh	Planet setures - A	Protocol TCP	Port 5060	SIP Entity 2 Communication Manager	Port 5060		Newson 1

6.6. Administer Routing Policies

Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

Under General:

- Enter an informative name in the Name field
- Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity to which this routing policy applies
- Under Time of Day, click Add, and then select the time range

The following screen shows the routing policy for Communication Manager.

Home /Elements / Routing / Routing Polici	les								
									Help ?
Routing Policy Details									Commit Cancel
Contract									
General	* ••								
l	* Name:								
	Disabled:								
	* Retries:	0							
	Notes:								
SIP Entity as Destination									
Select									
Select Name		FQDN c	or IP Addi	ess				Туре	Notes
		FQDN c		ess				Type CM	Notes
Name Communication Manager				ess					Notes
Name Communication Manager Time of Day				ess					Notes
Name Communication Manager				ess					Notes
Name Communication Manager Time of Day				ess					Notes
Name Communication Manager Time of Day (Add) Remove View Gaps/Overlaps 1 Item Refresh		10.10.9.		Fri	Sat	Sun	Start Time		
Name Communication Manager Time of Day Add Remove View Gaps/Overlaps 1 Item Refresh Ranking 1 Name Name 2 Name	10n Tu V V	10.10.9. e Wed	52	1	Sat	Sun	Start Time 00:00	CM	Filter: Enable

Heip ? Conmit Cancel * Name: External Disabled: Disabled:	Home /Elements / Routing / Routing	Policies									
* Name: External Disabled: * Retries: 0 Notes: SIP Entity as Destination Select: Sipera SDC 10.10.9.71 Gateway: Type Notes Sipera SBC 10.10.9.71 Gateway: Time of Day Add 1 Item Refresh Filter: Enable Filter: Enable	Routing Policy Details										
Disabled:	General										
Retries: O Notes:		* Name	e: Externa	al							
Notes: Type Notes: Select: Name FQDN or IP Address Type Notes Sipera SBC 10.10.9.71 Gateway Gateway Time of Day Item: Refresh Filter: Enable Filter: Enable 1 Item: Refresh Filter: Marking 1 Mane Mon Tue Wed Thu Fri Sat Start Time End Time Notes		Disabled	1: 🔲								
SIP Entity as Destination Select Type Notes Name FQDN or IP Address Type Notes Sipera SBC 10.10.9.71 Gateway Gateway Time of Day Kemove View Gaps/Overlaps Filter: Enable 1 Item Refresh Filter Sat Sun Start Time End Time Notes		* Retries	5: 0								
Name FQDN or IP Address Type Notes Sipera SBC 10.10.9.71 Gateway Time of Day Add Remove View Gaps/Overlaps 1 Item Refresh Filter: Enable Ranking 1 Mame 2 Mon Tue Wed Thu Fri Sat Sun Start Time End Time Notes		Notes	5:								
Time of Day Add Remove View Gaps/Overlaps 1 Item Refresh Filter: Enable Ranking 1 Name 2 Mon Tue Wed Thu Fri Sat Sun Start Time End Time Notes	Select	FQDN or IP /	Address						Туре	Note	15
Add Remove View Gaps/Overlaps 1 Item Refresh -<	Sipera SBC	10.10.9.71							Gateway	8	
Ranking 1 a Name 2 a Mon Tue Wed Thu Fri Sat Sun Start Time End Time Notes	Add Remove View Gaps/Ove	rlaps									
	1 Item Refresh		****	0.0000		1.0000	2 (2	- 22			
			Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
				101	2	121	1001	Dol:	00,00	22,50	Time Panes 34/7

The following screen shows the routing policy for the Session Border Controller.

6.7. Administer Dial Patterns

A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under General:

- In the **Pattern** field enter a dialled number or prefix to be matched
- In the Min field enter the minimum length of the dialled number
- In the **Max** field enter the maximum length of the dialled number
- In the **SIP Domain** field select **ALL** or alternatively one of those configured in **Section** 6.2

Under Originating Locations and Routing Policies, click Add. In the resulting screen (not shown), under Originating Location select ALL and under Routing Policies select one of the routing policies defined in Section 6.6. Click the Select button to save. The following screen shows an example dial pattern configured for the Session Border Controller which will route the calls out to the T-Mobile Vast Mobiel Integratie service.

Home /Elements / Routing / Dial Patter	rns					
Dial Pattern Details						Help ? Commit Cancel
General						
Emerge Emer	* Pattern: 00353 * Min: 5 * Max: 14 ergency Call: rgency Type: SIP Domain: -ALL- Notes:	M				
Originating Locations and Routing F Add Remove	Policies					Filter: Enable
	riginating Location otes	Routing Policy Name	Rank 2.▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Galway		External	0	Disabica	Sipera SBC	
Select : All, None						

The following screen shows the test dial pattern configured for Communication Manager. Note that the last six digits are not shown.

Home /Elements / Routing / Dial Patterns						
Dial Pattern Details					1)	Help ? Commit Cancel
General						
*	Pattern: 018nnnr	nn]		
	* Min: 9					
	* Max: 10					
Emerge	ency Call:					
Emergency	Priority: 1					
Emergen	ncy Type:					
SIP	Domain: -ALL-	×				
	Notes:					
Originating Locations and Routing Polic	cies					
Add Remove						
1 Item Refresh						Filter: Enable
Originating Location Name 1 Origin	nating Location s	Routing Policy Name	Rank 2 🛋	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Galway		Internal	0		Communication Manager	
Select : All, None						

6.8. Administer Application for Avaya Aura® Communication Manager

From the Home tab, select Session Manager from the menu. In the resulting tab from the left panel menu, select Application Configuration \rightarrow Applications and click New.

- In the **Name** field enter a name for the application
- In the SIP Entity field select the SIP entity for the Communication Manager
- In the **CM System for SIP Entity** field select the SIP entity for the Communication Manager

Select **Commit** to save the configuration.

lome /Elements /	/ Session Manager / A	pplication Configurat	ion / Applications		
					Help ?
Application	Editor				Commit Cancel
Application					
Name cm-app	p				
SIP Entity Comm	nunication Manager 🐱				
CM System for SIP CM In: Entity	stance 💙 🛛 Refresh	<u>View/Add</u> <u>CM</u> Systems		R.	
Description					
Application Att	ributes (optional)				
Name	Value				
Application Handle					
URI Parameters					
Application Me					
Enable Media Filteri	ng 🔲				
Audio	Video	Text	Match Type	If SDP Missing	
VEC		VEC	NOT EXACT N	ALL OW INC	

6.9. Administer Application Sequence for Avaya Aura® Communication Manager

From the left panel, navigate to Session Manager \rightarrow Application Configuration \rightarrow Application Sequences and click on New.

- In the **Name** field enter a descriptive name
- Under Available Applications, click the + sign in front of the appropriate application instance. When the screen refreshes, the application should be displayed under the Applications in this Sequence heading.

Select Commit.

Home	/Elements	/ Session Manager	/ Application Configuration / Application	Sequences	
App	plication	I Sequence E	ditor		Help ?
Appli	ication Seq	ience			
*Name	e cm	-app-seq			
Descri	iption				
	ve First		siP Entity	Mandatory	Description
	last)	<u>cm-app</u>	Communication Manager		
Selec	ct : All, None				
1 Ite	m Refresh				Filter: Enable
	Name		SIP Entity	Desc	ription
÷	<u>cm-app</u>		Communication Manager		

6.10. Administer SIP Extensions

SIP extensions are registered with the Session Manager and use Communication Manager for their feature and configuration settings. From the Home tab, select **User Management** from the menu. Then select **Manage Users** and click **New** (not shown).

On the **Identity** tab:

- Enter the user's name in the Last Name and First Name fields
- In the Login Name field enter a unique system login name in the form of user@domain (e.g. 2296@avaya.com) which is used to create the user's primary handle
- The Authentication Type should be Basic
- In the **Password/Confirm Password** fields enter an alphanumeric password

iome /Users / User Management / Manage Users	
	Help ?
New User Profile	Commit & Continue Commit Cancel
Identity * Communication Profile * Memb	ership Contacts
Identity 💌	
* Last Name:	
* First Name:	
Middle Name:	
Description:	
* Login Name:	2296@avaya.com
* Authentication Type:	Basic 💌
* Password:	
* Confirm Password:	•••••
Localized Display Name:	
Endpoint Display Name:	
Title:	
Language Preference:	×
Time Zone:	(+1:0)GMT : Dublin, Edinburgh, Lisbon, London, Casablanca

On the **Communication Profile** tab, enter a numeric **Communication Profile Password** and confirm it, then expand the **Communication Address** section and click **New**. For the **Type** field, select **Avaya SIP** from the drop-down menu. In the **Fully Qualified Address** field, enter an extension number and select the relevant domain from the drop-down menu. Click the **Add** button.

Identity * Communication Profile	* Membership	Contacts			
Communication Profile 🕏					
Communication Profile	Password: ••••••				
New Delete Done Cancel					
Name					
Primary					
Select : None					
	* Name: Primary				
	Default :		1		
Communication Addre	ss 🔹				
New Edit Delete					
Туре	Ha	ndle		Domain	
No Records found	Al-				
	Туре:	Avaya SIP 💌			
* Full	y Qualified Address:	2296	@ avaya.com	*	
					Add Cancel

Expand the Session Manager Profile section.

- Make sure the Session Manager check box is checked
- Select the appropriate Session Manager instance from the drop-down menu in the **Primary Session Manager** field
- Select the appropriate application sequence from the drop-down menu in the **Origination Application Sequence** field configured in **Section 6.9**
- Select the appropriate application sequence from the drop-down menu in the **Termination Application Sequence** field configured in **Section 6.9**
- Select the appropriate location from the drop-down menu in the Home Location field

* Deinsen: Cossien Manager	Session Manager 👻	Primary	Secondary	Maximum
* Primary Session Manager	Session Manager 🞽	3	0	3
Secondary Session Manager	(None)	Primary	Secondary	Maximum
gination Application Sequence	cm-app-seq 💌			
mination Application Sequence	cm-app-seq 👻			
Conference Factory Set	(None) 💌			
Survivability Server	(None)			
* Home Location	Galway 💌			

Expand the **Endpoint Profile** section.

- Select the Communication Manager SIP Entity from the System drop-down menu
- Select **Endpoint** from the drop-down menu for **Profile Type**
- Enter the extension in the **Extension** field
- Select the desired template from the **Template** drop-down menu
- For the **Port** field select **IP**
- Select the Delete Endpoint on Unassign of Endpoint from User or on Delete User check box
- Select **Commit** to save changes and the System Manager will add the Communication Manager user configuration automatically

CM Endpoint Profile 💌		
* System	CM Instance 💌	
* Profile Type	Endpoint 💌	
Use Existing Endpoints		
* Extension	Q 2296 Endpoint Editor	
* Template	DEFAULT_9630SIP_CM_6_2	
Set Type	9630SIP	
Security Code		
* Port	QIP	
Voice Mail Number	2002	
Preferred Handle		
Delete Endpoint on Unassign of Endpoint from User or on Delete User.	ut 🔽	
Override Endpoint Name		

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Session Border Controller. At the time of writing the Avaya Session Border Controller for Enterprise was badged as the Sipera E-SBC (Enterprise Session Border Controller) developed for Unified Communications Security (UC-Sec). The Avaya Session Border Controller for Enterprise is administered using the UC-Sec Control Center.

7.1. Access Avaya Session Border Controller for Enterprise

Access the Session Border Controller using a web browser by entering the URL https://<ip-address>, where <ip-address> is the private IP address configured at installation. Select the UC-Sec Control Center.



Log in with the appropriate credentials.

Sipera Systems LEARN - VERIEY - PROTECT	Sign in Login ID Password Sign in
The UC-Sec ™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks.	
Visit the Sipera Systems website to learn more.	

Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved.

7.2. Define Network Information

Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the A1 and B1 interfaces are used, typically the A1 interface is used for the internal side and B1 is used for external. Each side of the Avaya SBCE can have only one interface assigned. To define the network information, navigate to Device Specific Settings \rightarrow Network Management in the UC-Sec Control Center menu on the left hand side and click on Add IP. Enter details in the blank box that appears at the end of the list

- Define the internal IP address with screening mask and assign to interface A1
- Select **Save** (not shown) to save the information
- Click on Add IP
- Define the external IP address with screening mask and assign to interface B1
- Select **Save** (not shown) to save the information
- Click on System Management in the main menu
- Select Restart Application indicated by an icon in the status bar

UC-Sec Devices	Network Configuration Interface Configurati	ion		
P_V9				
		ss or its associated data require an ap	oplication restart before taking effect. Applic	cation restarts can be
	issued from <u>System Management</u> .			/
	A1 Netmask 255.255.0 A2 Netr	mask B1 Ne	mask 255.255.255.240 B2 Netmask	¢
	Add IP		Save Changes	Clear Changes
	IP Address	Public IP	Gateway	Interface
	IP Address	Public IP	Gateway 10.10.9.1	Interface

Select the Interface Configuration tab and click on Toggle State to enable the interfaces.

UC-Sec Devices	Network Configuration Interface Configuration		
SSCP-SBC1	Name	Administrative Status	
	A1	Enabled	Toggle State
	A2	Disabled	Toggle State
	B1	Enabled	Toggle State
	B2	Disabled	Toggle State

7.3. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces.

7.3.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings** \rightarrow **Signaling Interface** in the **UC-Sec Control Center** menu on the left hand side. Details of transport protocol and ports for the internal and external SIP signalling are entered here

- Select Add Signaling Interface and enter details in the pop-up menu
- In the Name field enter a descriptive name for the internal signalling interface
- For Signaling IP, select an internal signalling interface IP address defined in Section 7.2
- Select UDP and TCP port numbers, **5060** is used for T-Mobile
- Select Add Signaling Interface and enter details in the pop-up menu
- In the Name field enter a descriptive name for the external signalling interface
- For Signaling IP, select an external signalling interface IP address defined in Section 7.2
- Select UDP and TCP port numbers, **5060** is used for T-Mobile

UC-Sec Devices	Signaling Interface						
SCP_V9						Add Signaling Int	terface
			No. of the local division of the local divis		71.0.0	TI C D51-	
	Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
	Name Int_Sig	Signaling IP 10.10.9.71	5060	5060	ILS Poπ	None	1

7.3.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings** \rightarrow **Media Interface** in the **UC-Sec Control Center** menu on the left hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

- Select Add Media Interface and enter details in the pop-up menu
- In the Name field enter a descriptive name for the internal media interface
- For Media IP, select an internal media interface IP address defined in Section 7.2
- Select **RTP port** ranges for the media path with the enterprise end-points
- Select Add Media Interface and enter details in the pop-up menu
- In the Name field enter a descriptive name for the external media interface
- For Media IP, select an external media interface IP address defined in Section 7.2
- Select **RTP port** ranges for the media path with the T-Mobile SBC

UC-Sec Devices GSSCP_V9		edia interface will require an application restart b	efore taking effect. Application restarts can be	issued from
	System Management. Name	Media IP	Add Me Port Range	dia Interface
	Int_Med	10.10.9.71	35000 - 40000	2 X
	Ext Med	192.168.27.34	35000 - 40000	27

7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, the T-Mobile SBC is connected as the Trunk Server and the Session Manager is connected as the Call Server. To define server interworking on the Avaya SBCE, navigate to **Global Profiles** \rightarrow **Server Interworking** in the **UC-Sec Control Center** menu on the left hand side. To define Server Interworking for the Session Manager, highlight the **avaya-ru** profile which is a factory setting appropriate for Avaya equipment and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile** (not shown)

- In the Clone Name field enter a descriptive name for the Session Manager and click Finish in test SM9 was used
- Select Edit and enter details in the pop-up menu.
- Check the **T.38** box
- Change the Hold Support RFC to RFC2543 then click Next and Finish

In	iterworking Profile
	General
Hold Support	C None RFC2543 - c=0.0.0.0 C RFC3264 - a=sendonly
180 Handling	None O SDP O No SDP
181 Handling	None C SDP C No SDP
182 Handling	None C SDP C No SDP
183 Handling	None C SDP C No SDP
Refer Handling	
3xx Handling	
Diversion Header Support	E
Delayed SDP Handling	
T.38 Support	v
URI Scheme	© SIP C TEL C ANY
Via Header Format	© RFC3261 © RFC2543
	Back Next

To define Server Interworking for the T-Mobile SBC, highlight the previously defined profile for the Session Manager and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile** (not shown)

- In the Clone Name field enter a descriptive name for server interworking profile for the T-Mobile SBC and click Finish in test T-Mobile was used
- Select Edit and enter details in the pop-up menu
- Check the **T.38** box
- Select Next three times and Finish

BG; Reviewed:
SPOC 6/25/2012

7.5. Define Servers

Servers are defined for each server connected to the Avaya SBCE. In this case, the T-Mobile SBC is connected as the Trunk Server and the Session Manager is connected as the Call Server. To define the Session Manager, navigate to **Global Profiles** \rightarrow Server Configuration in the UC-Sec Control Center menu on the left hand side. Click on Add Profile and enter details in the pop-up menu (not shown)

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next**
- In the Server Type drop down menu, select Call Server
- In the IP Addresses / Supported FQDNs box, type the Session Manager SIP interface address which is the same as that defined on the Communication Manager in Section 5.2
- Check TCP and UDP in Supported Transports
- Define the TCP and UDP ports for SIP signalling, **5060** is used for T-Mobile
- Click **Next** three times then select the **Interworking Profile** for the Session Manager defined in **Section 7.4** from the drop down menu

The General tab on the resultant screen shows the IP addresses, TCP Port and UDP Port entered.

Global Profiles > Server Configuration: SM9 Add Profile) Call Server		Rename Profile	Clone Profile	Delete Profile
Profile	General Authentication Heartbeat Advance	ced			
SM9 Call Server		General			
T-Mobile Trunk	Server Type	Call Server			
	IP Addresses / FQDNs	10.10.9.61			
	Supported Transports	TCP, UDP			
	TCP Port	5060			
	UDP Port	5060			
		Edit			17

The Advanced tab on the resultant screen shows the Interworking Profile for the call server defined in Section 7.4.

Global Profiles > Server Configuration: SM9 (Call Server				
Add Profile			Rename Profile	Clone Profile	Delete Profile
Profile	General Authentication Heartbeat Advanced				
SM9 Call Server		Advanced			
T-Mobile Trunk	Enable DoS Protection				
	Enable Grooming				
	Interworking Profile	SM9			
	Signaling Manipulation Script	None			
	TCP Connection Type	SUBID			
	UDP Connection Type	SUBID			
		Edit			

Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved. To define the T-Mobile SBC as a Trunk Server, navigate to Global Profiles \rightarrow Server Configuration in the UC-Sec Control Center menu on the left hand side. Click on Add Profile and enter details in the pop-up menu (not shown)

- In the **Profile Name** field enter a descriptive name for the T-Mobile SBC and click Next
- In the Server Type drop down menu, select Trunk Server
- In the IP Addresses / Supported FQDNs box, type the IP address of the T-Mobile SBC (not shown)
- Check **TCP** and **UDP** in **Supported Transports**
- Define the TCP and UDP ports for SIP signaling, **5060** is used for T-Mobile
- Click **Next** three times then select the **Interworking Profile** for the T-Mobile SBC defined in **Section 7.4** from the drop down menu

The General tab on the resultant screen shows the IP addresses, TCP Port and UDP Port entered.

Global Profiles > Server Configuration: T-Mob	ile Trunk				
Add Profile			Rename Profile	Clone Profile	Delete Profile
Profile	General Authentication Heartbeat Advance	d			
SM9 Call Server		General			
T-Mobile Trunk	Server Type	Trunk Server			
	IP Addresses / FQDNs	84.241.227.55			
	Supported Transports	TCP, UDP			
	TCP Port	5060			
	UDP Port	5060			
		Edit	10		0.5

The Advanced tab on the resultant screen shows the Interworking Profile for the trunk server defined in Section 7.4.

Add Profil Profile	e General Authentication Heartbeat Advance	d	Rename Profile	Clone Profile	Delete Profile
M9 Call Server		Advanced			
T-Mobile Trunk	Enable DoS Protection	Г			
	Enable Grooming	Г			
	Interworking Profile	T-Mobile			
	Signaling Manipulation Script	None			
	TCP Connection Type	SUBID			
	UDP Connection Type	SUBID			

7.6. Define Routing

Routing information is required for routing to the Session Manager on the internal side and the T-Mobile SBC on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used. To define routing to the Communication Manager, navigate to **Global Profiles** \rightarrow **Routing** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Routing Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next**
- Enter the Session Manager SIP interface address and port in the Next Hop Server 1 field
- Select **TCP** for the **Outgoing Transport**
- Click Finish

Note: Unless default port 5060 is used, the port must be included in the next hop IP address.

Global Profiles > Routing: SM9 Call Server											
Add Profile	l				Rename P	rofile	C	lone Pro	file	Delete Pro	ofile
Routing Profiles			Clic	k here to add a description.							
default	Routing Profile										
SM9 Call Server		÷									
T-Mob Trunk Server									Add R	outing Rule	
	Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV		lgnore Route Header	Transport	
	1 *		10.10.9.61		V	Γ	Г			TCP	2

To define routing to the T-Mobile SBC, navigate to **Global Profiles** \rightarrow **Routing** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the T-Mobile SBC and click **Next**
- Enter the T-Mobile SBC IP address and port in the Next Hop Server 1 field
- Check the Next Hop in Dialog box
- Select UDP for the Outgoing Transport
- Click Finish

Global Profiles > Routing: T-Mob Trunk Server											
Add Profile					Rename F	Profile	С	lone Prof	ile	Delete Pro	file
Routing Profiles			Clic	k here to add a description.							
default	Routing Profile										
SM9 Call Server	6.059.	10							100306-000		
T-Mob Trunk Server									Add Ro	outing Rule	
	Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV		lgnore Route Header	Outgoing Transport	
	1 *		84.241.227.55		•	Г	Г	Г	Г	UDP	1

7.7. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten or next hop IP addresses can be used. As IP addressing was used in test instead of domain names, there was little requirement for topology hiding. IP addresses are translated to the Avaya SBCE external addresses using NAT. To define Topology Hiding for the Session Manager, navigate to **Global Profiles** \rightarrow **Topology Hiding** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next**
- If the required Header is not shown, click on Add Header
- Select **Request-Line** as the required header from the **Header** drop down menu
- Select the required action from the **Required Action** drop down menu, **Next Hop** was used for test

Note: The use of **Next Hop** results in the IP address being inserted in the host portion of the Request-URI as opposed to a domain name. If a domain name is required, the action **Overwrite** must be used for the **Request-Line** header with the required domain names entered in the **Overwrite Value** field. Different domain names could be used for the enterprise and the T-Mobile network.

Global Profiles > Topology Hiding: SM9									
Add Profile			Rename Profile	Clone Profile Delete Profile					
Topology Hiding Profiles	Topology Hiding Profiles Click here to add a description.								
default	Topology Hiding								
cisco_th_profile	lineder	Cathodia	Destas Astiss	Ourses with Mature					
SM9	Header	Criteria	Replace Action	Overwrite Value					
T-Mob Trunk	Request-Line	IP/Domain	Next Hop						

To define Topology Hiding for the T-Mobile SBC, navigate to **Global Profiles** \rightarrow **Topology Hiding** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for the T-Mobile SBC and click **Next**
- If the Request-Line Header is not shown, click on Add Header
- Select **Request-Line** as the required header from the **Header** drop down menu
- Select the required action from the **Replace Action** drop down menu, **Next Hop** was used for test
- If the Via Header is not shown, click on Add Header
- Select Via as the required header from the Header drop down menu
- Leave the **Required Action** at the default value of **Auto**
- If the Record-Route Header is not shown, click on Add Header
- Select **Record-Route** as the required header from the **Header** drop down menu
- Leave the **Required Action** at the default value of **Auto**

Global Profiles > Topology Hiding: T-Mob Trun	k			
Add Profile			Rename Profile	Clone Profile Delete Profile
Topology Hiding Profiles		Click he	ere to add a description.	
default	Topology Hiding			
cisco_th_profile	Header	Criteria	Replace Action	Overwrite Value
SM9	Via	IP/Domain	Auto	
T-Mob Trunk	Request-Line	IP/Domain	Next Hop	
	Record-Route	IP/Domain	Auto	
			Edit	

Note: Topology Hiding on the **Via** and **Record-Route** headers was required in test to replace the multiple entries for the enterprise equipment with a single entry for the SBC. This reduced the overall size of the SIP INVITE so that it was not fragmented.

7.8. Server Flows

Server Flows combine the previously defined profiles into an outgoing flow from the Session Manager to the T-Mobile SBC and an incoming flow from the T-Mobile SBC to the Session Manager. This configuration ties all the previously entered information together so that calls can be routed from the Session Manager to the T-Mobile SBC and vice versa. The information for all Server Flows is shown on a single screen on the Avaya SBCE.

C-Sec Devices	Subscribe	Flows Server Flows												
													Add	Flow
					Hover	over a row t	o see its de	scription.						
	Server Co	nfiguration: SM9 Call Se	rver											
	Priority	Flow Name	UF Gro		ort Remo		ed Signalin :e Interfac		End Point Policy Group	Routing Profile		File Transfer Profile		
	1	SM6_Call_Server	*	*	*	Ext_Sig	Int_Sig	Int_Med	default- Iow	T-Mob Trunk Server	SM9	None	0	×
	Server Co	nfiguration: T-Mobile Tru	ink											
	Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile		
	1	T-Mobile_Trunk	*	*	*	Int_Sig	Ext_Sig	Ext_Med	t-mob- low	SM9 Call Server	T-Mob Trunk	None		×

To define an outgoing Server Flow, navigate to **Device Specific Settings** \rightarrow End Point Flows.

- Click on the Server Flows tab
- Select Add Flow and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the outgoing server flow to the T-Mobile SBC
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 7.6**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the T-Mobile SBC defined in **Section 7.7** and click **Finish**

Priority	Flow Name	URI Group	Transport	Remote Subnet				End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile		
1	T-Mobile_Trunk	*	*	*	Int_Sig	Ext_Sig	Ext_Med	t-mob- Iow	SM9 Call Server	T-Mob Trunk	None	0	×

An incoming Server Flow is defined as a reversal of the outgoing Server Flow

- Click on the Server Flows tab
- Select Add Flow and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the incoming server flow to the Session Manager
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**
- In the **Signalling Interface** drop-down menu, select the internal SIP signalling defined in **Section 7.3**
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3**
- In the **Routing Profile** drop-down menu, select the routing profile of the T-Mobile SBC defined in **Section 7.6**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Session Manager defined in **Section 7.7** and click **Finish**

Priority	Flow Name	URI Group	Transport			Signaling Interface		End Point Policy Group	Routing Profile		File Transfer Profile			
1	SM6_Call_Server	*	×	*	Ext_Sig	Int_Sig	Int_Med	default- Iow	T-Mob Trunk Server	SM9	None	0	×	4

8. Service Provider Configuration

The configuration of the T-Mobile equipment used to support the T-Mobile Vast Mobiel Integratie service is outside of the scope of these Application Notes and will not be covered. To obtain further information on T-Mobile equipment and system configuration please contact an authorised T-Mobile representative.

9. Verification Steps

This section provides steps that may be performed to verify that the solution is configured correctly.

 From System Manager Home Tab, click on Session Manager and navigate to Session Manager → System Status → SIP Entity Monitoring. Select the relevant SIP Entity from the list and observe if the Conn Status and Link Status are showing as up.

							Help
	ntity, Entity Link Co	onnection Status					
nis page d	isplays detailed connection status fo	or all entity links from all Session Manag	ger instances to	a single SIP (entity.		
and a second second	ity Links to SIP Entity: Si nary View Refresh	pera Soc					Filter: Enable
Sumr	nary View	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Filter: Enable

2. From the Communication Manager SAT interface run the command **status trunk n** where **n** is a previously configured SIP trunk. Observe if all channels on the trunk group display **in-service/idle**.

status ti	runk 1		
		TRUNK (GROUP STATUS
Member	Port	Service State	Mtce Connected Ports Busy
0001/001 0001/002 0001/003 0001/004 0001/005	T00002 T00003 T00004	<pre>in-service/idle in-service/idle in-service/idle in-service/idle</pre>	no no no
0001/005 0001/006 0001/007 0001/008 0001/009	T00006 T00007 T00008	<pre>in-service/idle in-service/idle in-service/idle in-service/idle in-service/idle</pre>	no no no no
0001/010	T00010	in-service/idle	no

3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.

- 4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
- 5. Verify that the user on the PSTN can end an active call by hanging up.
- 6. Verify that an endpoint at the enterprise site can end an active call by hanging up.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise to T-Mobile Vast Mobiel Integratie service. The service was successfully tested with a number of observations listed in **Section 2.2**.

11. References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at <u>http://support.avaya.com</u>.

- [1] Installing and Configuring Avaya Aura® System Platform Release 6.2, March 2012.
- [2] Administering Avaya Aura® System Platform Release 6.2, February 2012.
- [3] Administering Avaya Aura® Communication Manager, Release 6.2, February 2012.
- [4] Avaya Aura® Communication Manager Feature Description and Implementation, February 2012, Document Number 555-245-205.
- [5] Implementing Avaya Aura® System Manager Release 6.2, March 2012.
- [6] Implementing Avaya Aura® Session Manager, February 2012, Document Number 03-603473
- [7] Administering Avaya Aura® Session Manager, February 2012, Document Number 03-603324.
- [8] Various Application Notes for the Avaya Session Border Controller for Enterprise, March 2012
- [9] RFC 3261 SIP: Session Initiation Protocol, <u>http://www.ietf.org/</u>

©2012 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and TM are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at <u>devconnect@avaya.com</u>.